epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

July 21, 2023

The Honorable Chuck Schumer
322 Hart Senate Office Building
Washington, D.C. 20510

Dear Leader Schumer:

We write to oppose the STOP CSAM Act, which has also been introduced as amendment #251to the National Defense Authorization Act.

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[1] EPIC recognizes the legitimate concerns about the distribution of child sexual exploitation material ("CSAM") online and supports efforts to reform Section 230 of the Communications Decency Act to force companies to comply with take-down requests. But EPIC also opposes efforts to undermine strong encryption. While some of the proposals in the STOP CSAM Act are laudable, others would threaten encryption and impose serious privacy and speech harms on internet users.

EPIC has two significant concerns with the STOP CSAM Act. First, the STOP CSAM Act endangers strong encryption by allowing a company's use of end-to-end and other encryption services to be a basis of liability and/or evidence of fault in cases involving CSAM. Second, the amendment raises significant privacy and speech concerns by requiring providers scan for certain online conduct and then report those who engage in such conduct to police. Such a scanning and reporting regime will disproportionately impact teenagers—particularly LGBT youth—who share sexually explicit photos of themselves at significantly high rates.

Providers Should Not Be Able to Ignore Reported CSAM

Section 230 should not protect providers who ignore requests to remove CSAM.[2] That is why EPIC has supported the SAFE TECH Act, which would reform Section 230 to allow child victims—and others whose intimate images are distributed without consent online—to obtain injunctions that require providers to remove offending materials.[3]

Some of the STOP CSAM Act's proposals to force providers to respond to take-down requests are laudable. EPIC supports the idea of requiring providers to create portals dedicated to

[1] EPIC, *About EPIC*, https://epic.org/about/
[2] Naomi Nix, *Meta Joins Porn Sites in Backing New Tool to Fight Revenge Porn*, Washington Post (Feb. 28, 2023), https://www.washingtonpost.com/technology/2023/02/28/meta-revenge-porn-take-it-down/.
[3] Sen. Mark. R. Warner, *Legislation to Reform Section 230 Reintroduced in the Senate, House* (Feb. 28, 2023), https://www.warner.senate.gov/public/index.cfm/2023/2/legislation-to-reform-section-230-reintroduced-in-the-senate-house.

receiving reports of CSAM and to respond to these reports in a timely manner. EPIC also supports providing child victims with new rights to seek redress should providers fail to adequately respond to their take-down requests.

If that were all the STOP CSAM Act did, we might be able to support it. But the STOP CSAM Act goes far beyond what is necessary to address the problem of providers ignoring take-down requests. By making providers liable for recklessly hosting or promoting or facilitating CSAM distribution, the Act threatens strong encryption—which is vital to privacy and security online—and, especially when combined with new reporting requirements, likely violates the Fourth Amendment.

The STOP CSAM Act Threatens Strong Encryption

EPIC has long supported strong encryption, like end-to-end encryption ("E2EE"), as a means to protect users, promote commerce, and ensure cybersecurity.[4] Congress should not pressure companies to abandon E2EE – but the STOP CSAM Act will do just that.

First, the Act would only prevent litigants from using provision of encryption services as an "independent basis" for provider liability. This may prevent suits against providers for facilitating or promoting CSAM distribution when the only allegation supporting this claim is that the provider uses strong encryption, but E2EE is usually combined with other design features—such as anonymity—that could be used as part of the basis of liability along with encryption.

Second, and perhaps more troublingly, the STOP CSAM Act explicitly allows E2EE to be used as evidence against providers in anti-CSAM suits. This would allow encryption to be used as evidence of fault. Good cybersecurity practices such as encryption should not lead to liability.

Third, the Act would add liability for reckless conduct that can be construed to include full E2EE. One provision would allow plaintiffs to sue providers or app stores for "the intentional, knowing, or *reckless* promotion or facilitation of conduct that violates" an anti-CSAM law. The provision allows suits against providers for "the intentional, knowing, or *reckless* hosting or storing of child pornography or making child pornography available to any person." Because the STOP CSAM Act explicitly allows E2EE to be used as evidence against providers for, e.g., determining fault, it is almost assured that plaintiffs and prosecutors will use these new causes of action to go after companies that did not know they were hosting CSAM simply because they provide E2EE and people used their services to host or distribute CSAM. The mere prospect of liability in these situations will lead providers to abandon E2EE.

Internet companies will abandon E2EE if they expect it to lead to massive liability. The STOP CSAM Act does just that. Providing strong encryption should not be allowed to form *any part* of the basis for liability against a provider or be used *in any way* as evidence in anti-CSAM suits. Because the STOP CSAM Act explicitly allows E2EE to be used as evidence against providers, EPIC opposes the Act.

[4] *See*, EPIC, *Encryption*, https://epic.org/issues/cybersecurity/encryption/.

The STOP CSAM Act Raises Serious Speech and Privacy Concerns

The STOP CSAM Act's expanded liability for reckless acts involving CSAM, combined with the Act's proposed expansion of obligations on providers to report CSAM activity, create a perfect storm of speech and privacy problems. The first set of provisions create duties to search for CSAM and CSAM-related conduct, while the second set create duties to report such conduct to police. The combination would transform providers into government agents and, as a result, provider searches would violate the Fourth Amendment. This would not only invade people's privacy, it would also jeopardize prosecutions of known CSAM. Forcing providers to search for nebulous conduct related to CSAM possession or distribution would also cause widespread privacy and speech harms.

The expanded civil liability in the STOP CSAM Act would create duties for providers to proactively look not only for CSAM but for other activities that can be construed as promoting or facilitating CSAM distribution. Current law only imposes liability when providers *know* of CSAM, but it does not require providers to look for CSAM. By lowering the bar for liability to reckless acts, the STOP CSAM Act compels providers to actively look for CSAM.

Because the STOP CSAM Act also imposes liability when a provider promotes or facilitates conduct that violates anti-CSAM laws, the Act also compels providers to look for other types of conduct related to the distribution of CSAM. Providers could not detect such conduct by using perceptual hash matching software like PhotoDNA because such software can only detect CSAM that is known and previously assigned a hash value. Instead, providers would have to build new tools that attempt to detect not just previously unknown CSAM but conduct that could lead to the distribution of CSAM. Such a tool might use machine learning to detect new instances of CSAM and patterns in conversations that could lead to CSAM distribution. Tools like this would severely infringe on people's privacy, infringe on protected speech, and would likely result in a significant increase in erroneous reports to police. Indeed, news stories about Google's AI CSAM detection tool show the impact on people whose images are erroneously flagged as CSAM – parents who sent images of their children to a doctor for diagnosis of health concerns have been reported to police and had their Google accounts permanently locked even after police determined that the images did not constitute CSAM.[5] Such false reports to police could have additional harmful effects, such as threatening a person's custody in their child.

Meanwhile, the new reporting requirements would force providers to report to the National Center for Missing & Exploited Children (NCMEC), who would then report to police, any instance not just of apparent CSAM but "planned or imminent" violation of anti-CSAM laws. A "planned or imminent" violation is vague and could encompass a wide swath of activity. The new reporting requirements, when combined with the duty to proactively search for CSAM and CSAM-related behavior, would result in people being reported to police for a broad range of online conduct, much

[5] Kashmir Hill, *A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal*, N.Y. Times (Aug. 21, 2022), https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html.

of which does not violate any laws. It would also turn providers into government agents, making the providers' searches violate the Fourth Amendment.[6]

Teenagers—particularly LGBT teenagers—will be disproportionately impacted by such a scanning and reporting regime. A substantial portion of teenagers today send or receive sexually explicit text messages and photos, a behavior known as "sexting." Over 19 percent of adolescents report having sent a sext, 34.8 percent have received one, and 14.5 percent have forwarded a sext without consent.[7] Studies show that LGBT youth are more likely than their heterosexual peers to engage in sexual conversations and share sexual pictures online.[8] Experts say that consensual teen sexting is "not known to be initially harmful to either party" and is not likely to be remedied by police but "rather is a health and education issue that is better addressed at home, in schools, and in primary care." [9] Prosecuting teens for sexting is also contrary to the legislative intent behind CSAM laws.[10] Yet, all of these teens would be at risk of prosecution in the 23 states that prosecute teenagers for violations of CSAM laws.[11] Even in states that do not prosecute teenagers for CSAM, referral to police can cause embarrassment, stigma, and even potential violence, particularly for LGBT youth whose families and community were not previously aware of or are not accepting of their sexual identity.

Even under the current reporting regime—which only requires providers send a CyberTip if they know of an apparent violation of anti-CSAM laws—the STOP CSAM Act's attempt to lower the bar for liability to reckless acts would likely violate the Fourth Amendment. Creating a duty to search for CSAM, combined with a duty to report the person who possesses that CSAM, would transform providers into government agents. This would endanger prosecutions for possessing or

---

[6] Courts have held that providers are not government agents in cases where they actively search for and report CSAM because providers take on these searches voluntarily. If Congress placed a duty on providers to conduct such searches, courts would likely find otherwise. *See, e.g.*, *United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012) (provider not government agent because the law does "not impose any obligation to search for child pornography, merely an obligation to report child pornography of which [an ESP becomes] aware," and ESPs "voluntarily choose" to monitor their platforms "pursuant to [their] own internal policy" and are not "compelled" by the government); *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010) (provider not a government agent because there is no "congressional preference for monitoring" and the overall statutory scheme "in no way encourages surreptitious searches"); *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) (provider not government agent because the statutory scheme does not dictate "whether or how [an ESP] should scan its users' [data]").

[7] Camille Mori *et al.*, *Are Youth Sexting Rates Still on the Rise? A Meta-Analytic Update*, 70 J. Adolescent Health 531, 531-39 (2022), *available at* https://pubmed.ncbi.nlm.nih.gov/34916123/.

[8] Ybarra, M. L., & Mitchell, K. J. (2016). *A National Study of Lesbian, Gay, Bisexual (LGB), and Non-LGB Youth Sexual Behavior Online and In-Person*, Archives of Sexual Behavior, 45(6), 1357-1372, https://pubmed.ncbi.nlm.nih.gov/25894645/.

[9] *See* Victor Strasburger, Harry Zimmerman & Jeff Temple, *Teenagers, Sexting, and the Law*, 143 Pediatrics 1, 3 (2019), https://publications.aap.org/pediatrics/article/143/5/e20183183/37112/Teenagers-Sexting-and-the-Law?.

[10] Joanna R. Lampe, *A Victimless Sex Crime: The Case for Decriminalizing Consensual Teen Sexting*, 46 U. Mich. J. L. Reform 703 (2013), *available at* https://repository.law.umich.edu/mjlr/vol46/iss2/18; Robert Mummert, *Sexting and the Law: How Lack of Reform in California Puts Teenagers in Jeopardy of Prosecution Under Child Pornography Laws Enacted to Protect Them*, 38 W. St. U. L. Rev. 71 (2010).

[11] Strasburg et al., *supra note 10*.

distributing actual CSAM, as such prosecutions currently rely on the theory that providers are acting voluntarily in searching for CSAM on their services.[12]

The STOP CSAM Act threatens encryption and imposes serious privacy and speech harms on internet users. EPIC urges you to reject this proposal, whether as a standalone bill or an amendment to the NDAA.

Thank you for your attention to this issue.

Sincerely,

Megan Iorio
Megan Iorio
EPIC Senior Counsel

Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Deputy Director

[12] *See supra* note 6.